STEPS TO RAPIDLY IMPROVE THE PERFORMANCE OF CA IDENTITY MINDER (IM)

ALAN BAUGHER

2013-12-03

BASIC / QUICK TACTICAL WINS

CHECKLIST

Basic / Quick Tactical Wins

Effort = < 1 - 2 hour(s) per objective

15 objectives

- TP cleanup
- Screen Indexes
- IM -> IMPS mappings
- JIAM Cache
- InMemoryEvaluation
- IMPS Logging reductions
- User Sync Options
- Tuning JVM guidelines
- SM LDAP Directory Operations
- CA Directory DSA Resizing / Update
- Linux Entropy (SM/JCS/WebAppServer)
- ADS/Exchange Timeout
- Validate Load Balancing
- AV Exclusion
- Disable IMPS NT Services

Managing & Correcting Error Messages

Effort = 1 day – 2 weeks for all areas

3 areas

- Web Application Server Logs
- IMPS Server Logs
- SM & Directory Logs

Advance Training

Effort = 1-4 week(s)

2 objectives

- Sandbox Lab
- OJT expansion of solution & training sessions

Document Business Logic in PX/IdentityPolicies/Provisioning

BASIC / QUICK TACTICAL WINS 01

- **Impact: High value/minimal effort to implement**
- Description: Clean up the task persistence database / tables {Keep it slim}
  - Do NOT let this table go for weeks/months without clearing out the old data.
  - Every time a user logins in or performs an action, IM reads this database & associated tables
  - When the records are over a million plus rows, degradation of performance will result.
  - There is an OOTB IM task made for to address this issue.
  - Decide on how much data must to be kept for active usage of the IM solution.
    - Most clients will retain a minimum of three (3) to four (4) weeks of data
    - Why? Because if there are any workflow events; anyone who goes on vacation for two (2) weeks, will see the approval request when they get back. This assumes the workflow remains active; and has not already been delegated or has a built-in SLA to advance to another approver.
  - Decide if information is to be retains for audits or reports
    - Check box on the "Clean up task" allows for data to be "moved" instead of deleted, to an archive task persistence table.
    - Few clients leverage this, as there is an audit table in place for long term data to be retained.
      - Task audit checkbox MUST be turned on to leverage.
  - If possible, perform a database row count on the table tasksession12_5, before and after clean up task has executed. This will give the admin a reasonable metric how long a clean up operation will take to move from millions of rows to a goal of 100,000 of rows. Confirm that tasksession_id is a GUID entry. Perform an unique check on tasksession_id between TP and TPA using SQL compare of the tasksession_id columns.
  - Advance note: If this site has more data coming into the IM solution via external TWES calls than can be managed by daily OOTB clean-up task, see the advance section.
- Actions: Login to IM User Console as a system admin; and schedule the TP clean up on a daily scheduled basis to remove any non-active task older than 14-21+ days.
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1031429.html?
  - https://communities.ca.com/web/ca-identity-and-access-mgmt-distributed-global-user-community/message-board/-/message_boards/view_message/97528088;jsessionid=FB13691C0CC99A77451A23602B8A869C.usilap722?&#p_19

BASIC / QUICK TACTICAL WINS 02

- **Impact: High value/Requires DBA skill set to implement**
- Description: Add Indexes to high usage IM screen tables
  - *Post-install task;* Only run AFTER an IME is created.
  - Object store tables IM_SCREEN_LD & IM_SCREEN_FIELD_LD
  - Pre-built Scripts included in the IM Tools Folder under samples
    - /opt/CA/IdentityMinder/IAM_Suite/IdentityManager/tools/samples/ObjectStore/
  - Requires a DBA or access to the IM tables as the db owner to execute scripts
  - Improve usability of screens loading
    - From 10's seconds to less than 5 seconds
- Actions: Login to IM Database GUI or CLI Console; execute IM scripts; log off IM Database GUI or CLI Console; done.
    - Example with Oracle XE DB:
      - su - oracle
      - sqlplus idmdba001/Password01
      - SQL> @/opt/CA/IdentityMinder/IAM_Suite/IdentityManager/tools/samples/ObjectStore/objectstore_db_oracle.sql
      - SQL> exit
- Reference:
  - /opt/CA/IdentityMinder/IAM_Suite/IdentityManager/tools/samples/ObjectStore/readme.txt

BASIC / QUICK TACTICAL WINS 03

- **Impact: Medium value/minimal effort to implement**
- Description: Remove unnecessary default corporate to provisioning mappings
  - OOTB mappings of IM Well-Known User attributes are:
    - %ADMIN_OF%
    - %ADMIN_ROLE_CONSTRAINT%
    - %CERTIFICATION_STATUS%
    - %DELEGATORS%
    - %IDENTITY_POLICY%
    - %LAST_CERTIFIED_DATE%
    - %PASSWORD_DATA%
    - Note:
      - These default settings were retained for a few clients that were moving from an pure provisioning deployment model to a corporate store model+ provisioning deployment model, to avoid issues during upgrades with any custom business logic.
      - This will remove unnecessary sync operations and corresponding IM call back operations for these attributes.
      - These setting are not required for new deployments.
  - Reduce impact for * queries that may impact other users and processes
    - By default, the value for maximum rows and page size is unlimited for existing directories. For new directories, the value for maximum rows is unlimited and the value for page size is 2000.
- Actions:
- Login to the IME Management console; Select the IME; select Advance Settings\Provisioning; under the section “Attribute Mappings”; remove the selected well-known attributes defined above.
- Update Directory.xml settings

BASIC / QUICK TACTICAL WINS 04

- **Impact: Medium value/minimal effort to implement**
- Description: Enabled IMPS Cache
  - Improve performance when look-ups are required, as a part of an IM task, to query the provisioning server for a user.
  - Reduce network overhead & false negative message in WAS logs about missing ID from cache
- Actions: Login to the IME Management console; Select the IME; select Advance Settings\Miscellaneous
  - Create two (2) tokens/properties with the following values:
    - *JIAMCache=true*
    - *JIAMCacheTTL=86400*
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?384757.html?

BASIC / QUICK TACTICAL WINS 05

- **Impact: Medium value/minimal effort to implement**
- Description: Enabled IM Memory Evaluation for login authorizations
  - Improve performance during & after login, when IM queries on a user's IM access from the IM corporate user store.
  - Reduce sequential ldap queries by using case sensitive cache feature.
    - If the setting of value =1 causes issue in the IME; use the other value to set non-case sensitive caching, value =3.
- Actions: Login to the IME Management console; Select the IME; select Advance Settings\Miscellaneous
  - Create a token/property with the following value:
    - *UseInMemoryEvaluation =1*
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?592744.html?

BASIC / QUICK TACTICAL WINS 06

- **Impact: High value/minimal effort to implement**
- Description: Disable excessive logging at the mid-tier components, e.g. Provisioning Server (IMPS)
  - Default logging level for transactions is set to level = 7 upon initial install
    - This log level captured all searches as well as update to the IMPS server and to endpoint managed by the IMPS server in the etatrans* logs.
    - Most client only require monitoring of create/update/delete transactions
    - CA support requests and requires that when support tickets are open, that a use-case is executed when the log level is set to level =7.
    - Recommendation is to lower the log level to **level =3** unless actively working a CA support ticket or attempting to isolate an issue.
    - Improve I/O performance and lower disk usage of IMPS etatrans* logs.
    - Improve IM performance when any IM task requires communication to the IMPS server and/or managed endpoints.
- Actions: Login to the IM Provisioning Manager GUI; Select System Tab; Select Domain Configuration button; Select Transaction Log; Select Level; Modify default value from 7 to 3; click apply; done. (no need to bounce services)
- Reference:
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?237642.html

BASIC / QUICK TACTICAL WINS 07

- **Impact: High value/minimal effort to implement**
- Description: Disable user sync for select IM tasks
  - Task User Sync Option has three (3) settings:
    - **On Task Completion**
      - Mandatory sync of all delta user attributes between IMCD and IMPS/PD when task completes (aka "Self-Healing")
    - **On Every Event**
      - Only sync the delta attributes in task/profile, but executes multiple times until the task completes.
    - **Off**
      - This task will not trigger user synchronization.
      - Used for tasks that do NOT required to be pushed/sync to IMPS, e.g. update questions.
  - OOTB IM tasks for create/modify/delete use-cases will have the default user sync option enabled to run "On Task Completion"
    - Recommend disable user sync option for default self-service task to update security questions and answers.
      - Improve performance of submission of questions/answers by preventing IM from trying to sync user's attributes that are not manage of this self-service task.
    - Use "OnEveryEvent" to limit use-case of task to only sync user attributes within the task's profile.
    - Other Tasks that may be adjusted: Prov Modify User, Prov Create User and Prov Delete User
- Actions: Login to the IM User Console; select Roles and Tasks; select Modify Task; select the IM Task by name; under Profile select User Synchronization; set to Off; test use-cases; ensure no issues or unexpected behavior; done.
- Reference:
  - https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?599193.html
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?AdminTaskProcessing.html
  - https://support.ca.com/cadocs/0/CA%20IdentityMinder%20r12%206-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?ConfigureAutomaticUserSynchronization.html

BASIC / QUICK TACTICAL WINS 08

- **Impact: High value/minimal effort to implement**
- Description: Update JVM options to improve memory, garbage collection, and ldap/s call performance.
- JVM Tuning {Aimed at JBOSS web application server; review for WebSphere & WebLogic frameworks}
  - Consider and fine tune the following JVM setup parameters :

  - # Memory Tuning for x64 / *– if using a 64 bit JVM, start at 2048m minimum and add the –d64 switch for linux/unix os (Note: IM Web App uses about 800MB when it starts)*
    JAVA_OPTS="$JAVA_OPTS –Xms2048m –Xmx4096m“

  - # Used to address performance with a WAS's JVM communicating to LDAP over SSL. Known issue with all WAS (JBOSS/WebLogic/WebSphere)
    May impact BLC
  - JAVA_OPTS="$JAVA_OPTS -Dcom.sun.jndi.ldap.connect.pool.protocol=plain\tssl Dcom.sun.jndi.ldap.connect.pool.debug=fine -Dcom.sun.jndi.ldap.connect.timeout=5000 -Dcom.sun.jndi.ldap.connect.pool.maxsize=300 -Dcom.sun.jndi.ldap.connect.pool.prefsize=10"

  - # Garbage collection is important. These are good baseline settings but will need to be tuned
  - JAVA_OPTS="$JAVA_OPTS -Dsun.rmi.dgc.client.gcInterval=3600000 -Dsun.rmi.dgc.server.gcInterval=3600000 -XX:+AggressiveOpts -XX:+AggressiveHeap -XX:+UseParallelGC"

  - # The below options are great for applications with a lot of looping code (such as IM)
  - JAVA_OPTS="$JAVA_OPTS -XX:CompileThreshold=10000"
  - JAVA_OPTS="$JAVA_OPTS -XX:+UseOnStackReplacement"

  - # The below is good for applications with many classes and intensive bootstraps
  - JAVA_OPTS="$JAVA_OPTS -XX:PermSize=128m -XX:MaxPermSize=256m -XX:ReservedCodeCacheSize=128m"

  - # The below dictates how the JVM will page in it’s heap. Use 4m or 16m pages in windows, 256m for Linux. Ensure that the heap size is evenly divisible by the page size. Windows OS may require GPO to be updated to allow service account to use “LargePages” memory feature.
  - JAVA_OPTS="$JAVA_OPTS -XX:+UseLargePages -XX:LargePageSizeInBytes=16m“

  - # The below address entropy challenge on headless/virtualized servers where entropy may be depleted and appears to halt the web app server
  - JAVA_OPTS=“$JAVA_OPTS -Djava.security.egd=file:/dev/./urandom"


D:\vmware\
jvm.txt


D:\run.bat

BASIC / QUICK TACTICAL WINS 09

- **Impact: High value/minimal effort to implement**
- Description: IM when integrated with SM, has all user directory authentication operations routed through SM. Update SM pool of Directory connections to increase number of fixed connections to improve performance for LDAP calls
- Within the SiteMinder WAM UI or FSS UI, select the User Directory
  - Edit the LDAP Directory Failover and Load Balancing Setup
  - Add the SAME LDAP server multiple times to the dialog box.
    - If using CA Directory start with 10 connections before starting performance query with CA IME.
      - Use the IM task for View or Modify User to see a difference
        - » Combined with the Screen Index Update, there will be a noticeable difference.

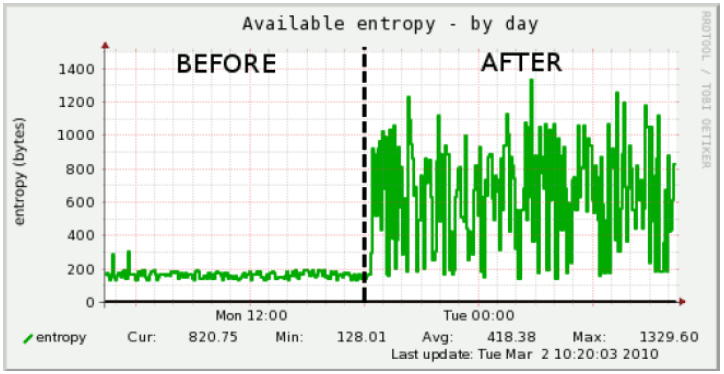
- Ref: https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?268042.html
- Additional Ref. for setting page limits:
- https://supportcontent.ca.com/cadocs/0/CA%20IdentityMinder%2012%206%202-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?268090.html

BASIC / QUICK TACTICAL WINS 10

- **Impact: Med value/minimal effort to implement**
- Description: CA Directory's DSA for IMPD / IMCD / Siteminder PolicyStore/KeyStore/SessionStore are typically setup with large memory sizes to accommodate expected or estimated (SWAG) growth.
- Sometimes the sizes used are an order of magnitude too large.
  - The process time that CA directory uses to manage the memory space and write to disk more excessive than is required.
  - The RAM space may be better used for other DSA on the server that need the space to grow.
  - The below process discuss how to identity the correct data size of the DSA and how to decrease or increase as needed.
- Design:
  - Review the DSA sizes defined in the DXHOME\config\servers*.dxi file
  - Perform a dump of the DSA data using dxdumpdb command for each DSA on a server.
    - dxdumpdb -f DSA_output.ldif DSA_Name
  - Review the size of the DSA's LDIF
    - This will give a good estimate of what the memory size is being used currently, as this size will be used as a base to estimate resizing needs.
    - DSA guideline for sizing should be roughly a minimal of 2.5x times the size of the LDIF file:
      - DSA's LDIF = 10 MB => DSA size = 25 MB => System needs 1 GB of RAM
      - DSA's LDIF = 2000 MB => DSA size = 5000 MB => System needs 8 GB of RAM, as 4 GB RAM would not be enough to allow the DSA to start.
    - If the DSA LDIF is near the current size of the DSA or within the 2.5x sizing guideline, then the DSA should be resize "upward" for growth.
      - Update the DXI file with new size; then stop DSA; Use the command: dxextenddb dsaname; restart DSA; They system will auto-resize the DSA data file.
      - https://supportcontent.ca.com/cadocs/0/CA%20Directory%20r12%200%20SP11-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?917385.html
- Action:
  - Downsizing a DSA's datastore:
    - 1. stop the DSA {dxserver stop dsaname}
    - 2. Dump the datastore to LDIF: "dxdumpdb -f {filename.ldif} dsaName"
      - example: dxdumpdb -f democorp.ldif democorp
    - 3. Edit the DSAs initialization file to edit the "dxgrid-db-size" to reduce it to the new size, and save the file {$DXHOME\dxserver\config\servers\dsaname.dxi}
    - 4. Reload the data using DXloaddb - "dxloaddb -s dsaName ldif-filename.ldif"
      - example: dxloaddb -s democorp democorp.ldif
    - 5. Start the DSA. {dxserver start dsaname}
  - Upgrade to CA Directory r12sp12 (10x faster than prior release) + Use included LoadBalancing features

BASIC / QUICK TACTICAL WINS 11

- **Impact: High value/minimal effort to implement**
- Description: Web App Servers (JBOSS/Weblogic/Websphere), IM w/FIPS, IM JCS service, CA Siteminder, & CA Directory may be deployed on RHEL/Linux; and performance for startup of services or connection to LDAP/S userstore may be lengthy due to low entropy on “headless virtual servers”.
- Background:
  - Encryption solutions need to have an random pool available from an OS to ensure the cryptography seed routines are secure.
  - Web Server with SSL server certificates, Client certs used between solution components, or any other solution that performs encryption.
  - Solutions that perform encryption on-the-fly are greatly affected by a low random noise pool.
  - Physical system can “fill” the entropy pool by direct interaction (mouse/keyboard), but on a headless server or virtual server with SSL/encryption traffic, the entropy pool can be drained faster than the system can replenish the data.
- Action: (SEE ENTROPY NOTES ON CA Community Site for further details)
  - DEV/TEST/QA (NON-PROD)
  - Use Software fix to address by replacing the device driver with the pseudo device driver
    - Rngd Toolset / Config Fix: vi /etc/sysconfig/rngd to contain:
      - # Add extra options here
      - EXTRAOPTIONS="-r /dev/urandom“
      - service rngd start & chkconfig rngd on
    - For JVM only
      - -Djava.security.egd=file:/dev/./urandom
  - PROD
    - Review adding hardware entropy generators + RNGD service.
    - Use HAVEGED entropy generator (processes/clock as input)



Reference:

https://support.ca.com/cadocs/0/CA%20SiteMinder%20r12%205-ENU/Bookshelf_Files/HTML/idocs/index.htm?toc.htm?1865112.html?zoom_highlight=random
http://en.wikipedia.org/wiki/Entropy_(computing)
http://tuxhelp.org/doku.php%3Fid=redhat:rngd:rgnd_init_script.html
http://www.linuxfromscratch.org/hints/downloads/files/entropy.txt

BASIC / QUICK TACTICAL WINS 12

- **Impact: High value/minimal effort to implement**
- Description: CA IM with provisioning may experience performance delays when provisioning AD accounts with Exchange mailboxes due to the OOTB limit of eighteen (18) concurrent sessions to Exchange via Powershell APIs; and if the delay is longer than the CA IM's CAM component timeout setting, the AD account will fail to be created.
- Background:
  - When an AD account is created, it is two (2) separate processes that occur very quickly, but may not be replicated as quickly. The AD account is first created with it's profile in a suspended state, then immediately after the account is created, AD then activates the account.
  - When creating an Exchange mailbox, the Exchange server has it's own list of AD Domain Controllers that it communicates to. These are the DC that Exchange uses to search for an AD account upon creation of the mailbox. If the AD account does not exist or is in a suspended status, the Exchange creation process will fail.
  - The CA IM AD Exchange Agent process, called by a AD service account, has default timeout settings set to create an Exchange mailbox. The IM agent on the Exchange server will use the Exchange APIs to check if the AD account exists and is in an active status before sending the create process to the Exchange server. If the AD account does not appears or show as active in the default timeout window, then the process will fail.
  - To address this issue and improve performance and reliability, the following changes are recommended.
- Actions:
  - On Exchange Server
    - Service account used to create Exchange mailbox has "Exchange Organization Administrator" Group assigned.
      - The CA CAM NT service should be setup to run under this ID
    - Increase the throttle sessions to 100 to accommodate IM bulk feeds that are sent in batches with a batch switch of 500.
      - 1. Exchange Admin may create a new Throttling policy to be used by select user accounts

        Example: New-ThrottlingPolicy MaxPowershell -PowerShellMaxConcurrency 100
      - 2. Exchange Admin would then apply this new throttling policy for the IM service account on the Exchange server.

        Example: Set-Mailbox "User Name" -ThrottlingPolicy MaxPowershell
    - Update Windows Registry Key for CA IM Exchange Agent from default of 60 seconds to **600** seconds
      - HKEY_LOCAL_MACHINE\SOFTWARE\ComputerAssociates\Identity Manager\Ex2k7AgentTimeout
    - Add the environmental variable **eTrustIM_RUS_Delay_Seconds** and add a value of **3** (seconds) [5x = 15 seconds]
  - On IMPS (IM Provisioning Server with CCS service)
    - Add the environmental variable **ADS_CONFIRM_MAILBOX = 600** (seconds)
    - Add the environmental variable of **ADS_E2K_SEND_DC** = **1** (on).
    - Add the environmental variable of **ADS_FAILOVER** = **1** (on) & pick only FAST DC on the ADS Endpoint Failover TAB
      - Note: we ALWAYS want the primary ADS DC endpoint to be the "PDC emulator" (this addresses password replication challenges within the AD domain)

BASIC / QUICK TACTICAL WINS 13

- **Impact: High value/minimal effort to implement**
- **Description:** The IM solution may be deployed in an high availability configuration with J2EE clustering with supported web servers that integrate with the J2EE web application servers; and with hardware load balancers. If the configurations are not correct, only a single stack may be used, and therefore the solution would not scale as expected. Typically, the J2EE platforms will be configured with "round-robin" as the load balancing feature for each transaction.
- The other tier to check for proper load balancing is the data tier: Directory for the corporate user store & Database for the IM object/TP store.
- **Actions:**
  - Monitor on each J2EE JVM the "used memory", when a bulk task is executed.
    - If the configuration is correct, then each transaction will be load balanced between each J2EE JVM; and reflected in the memory used of the JVM. If not configured correctly, only the first JVM will show activity.
    - To assist with analysis, a PX rule may be created to monitor the CREATE USER task, to write out to the web app log, with a notification message about the new userid. These results can be pulled from each web app server, to validate the load is being properly load balance by number of creations.
  - Monitor the queries to the directory to ensure that all directory servers are being utilized during login events and when data needs to be pulled or compared.
    - For updates, validate that one or selected directory servers, "designated as updated servers" are responsive enough to scale for password changes and other use-cases.
  - Monitor the database(s) used by IM solution
    - Using native or 3rd party tools, ensure that no query or update takes longer than 100 msec.
    - Ensure that the prior tactical suggestion of adding indexes to the IM SCREEN tables has been accomplished.
    - Validate underlying disc and NICs of the database servers are not a bottle neck for performance for database while it replicates data across a LAN or WAN for the remote database clusters.

BASIC / QUICK TACTICAL WINS 14

- **Impact: High value/minimal effort to implement**
- **Description:** The IM solution may be deployed on an OS with AntiVirus. The AntiVirus solution may be causing a performance hit to IM processes and folders during runtime.
- The IM processes and log folders are well known; and may be scanned on a daily basis, the business risk is minimal to exclude these processes and log folders from the RealTime AV Monitor.
- Use Microsoft SysInternal Tool, Process Explorer, to identify all IM processes on Windows OS
- **Actions:**
  - Update AV exclusion for IM processes and IM log folders
    - IMPS Server
      - Processes
        - im_ps.exe
        - im_ccs.exe
        - jcs.exe
        - Javaw.exe
        - dxserver.exe
        - cam.exe
        - caft.exe
        - etadmin.exe
    - IMWA Server
      - Processes
        - Java.exe
        - W3wwp.exe (MS IIS)
        - LLAWP.exe (SM WA)
        - Dxserver.exe
    - IMCD/IMPD
      - Processes
        - Dxserver.exe
        - Dxadmind.exe
    - SMPS
      - Processes
        - Smpolicysrv.exe
        - Service_policysrv.exe
        - Java.exe
        - Service_monsrvr.exe
        - Dxserver.exe
    - IMPS Server
      - Log Folders
        - D:\Program Files (x86)\CA\IdentityManager\ProvisioningServer\logs
        - D:\Program Files (x86)\CA\Identity Manager\Connector Server\logs
        - D:\Program Files\CA\Directory\dxserver\logs
    - IMWA Server
      - Processes
        - Web Application Server Logs
        - Web Server Logs
        - Web Agent Logs
        - D:\Program Files\CA\Directory\dxserver\logs
    - IMCD/IMPD
      - Processes
        - D:\Program Files\CA\Directory\dxserver\logs
    - SMPS
      - Processes
        - D:\Program Files\CA\siteminder\log
        - D:\Program Files\CA\Directory\dxserver\logs

BASIC / QUICK TACTICAL WINS 15

- **Impact: Low value/minimal effort to implement**
- **Description:** The IM solution provides a centralized log forwarding process for the IMPS tier. This centralized forwarding of log events may be sent via SNMP to a centralized console.
- If no SNMP forwarding is enabled, then the five (5) NT services for this service may be changed from auto-start to manual or disabled. The performance gain is slight, but as this component defaults its installation to the primary OS drive "C:\", this will offer relief for OS I/O operations.
- **Actions:**
  - Update Windows NT services for the five (5) CA Enterprise Common Services used for centralized logging to SNMP consoles. Reset from auto-start to manual or disabled.
    - Enterprise Common Services (Transport)
    - Enterprise Common Services GUI Framework
    - Enterprise Common Services Log Daemon
    - Enterprise Common Services Store-And-Forward Manager
    - Enterprise WorldView

MANAGING & CORRECTING ERROR MESSAGES

MANAGING & CORRECTING ERROR MESSAGES - 01

- **Impact: High Value / Medium Difficulty**
- Description: Create Goal for **No Error Message(s)** in Web Application Logs
  - This is the hidden performance challenge
  - After the install or anytime, pull the current full workday log from all web application servers of the cluster.
  - Edit the logs to ensure the server hostname, if missing, is added to the logs, after the date-time stamp
  - Join these files together into one new large file & sort by time stamp
  - Assumption: No common error console currently exist to be leveraged, instead.
- Actions:
  - Identify all error messages, e.g. strings with "ERROR"
  - Categorize and count error messages
    - Infrastructure, e.g. OS, Java, Database, Network
    - Product, e.g IM support with version of Infrastructure
    - Business Logic, e.g. PX Rules/Identity Policies/Custom BLTH/LAH/EL
  - Triage & determine which errors require CA Support Tickets or 3rd party vendor for product or unknown issue. Spend no more than 10 minutes on each issue to triage.
  - Open internal tracking list for CA and non-CA support Tickets
    - Assign resources to issue to resolve or work the issue
    - Tickets should be
      - Resolved (date of fix and deployment to QA/Stage/Model Env. and then when to production Env.),
      - Postponed (low impact),
      - Marked for resolution in confirm service pack (low-medium impact)
      - Escalated for CA support if CA Support ticket resolution not feasible in project time (high impact)
      - Escalated for internal management if internal resources resolution not feasible in project time (high impact)
  - Active Monitoring of Web Application Logs
    - May update log4j to separate IM application events from Web Application Server events
    - May use IM dynamic logging.jsp page to assist with debugging business logic

MANAGING & CORRECTING ERROR MESSAGES - 02

- **Impact: High Value / Medium Difficulty**
- Description: Create Goal of No Error Message(s) in Provisioning Server (eta), IAM CS (log4j) & Endpoint Logs (sa & ADS)
  - This is the hidden performance challenge
    - After the install or anytime, pull the current full work day ETA logs from all provisioning servers
    - Edit the logs to ensure the server hostname, if missing, is added to the logs, after the date-time stamp
    - Join these files together into one new large file & sort by time stamp
    - Assumption: No common error console currently exist to be leveraged, instead.
- Actions:
  - Identify all error messages, e.g. strings with "ERROR"
  - Categorize and count error messages
    - Infrastructure, e.g. OS, Java, Database, Network
    - Product, e.g IM support with version of Infrastructure
    - Business Logic, e.g. IMPS Account Templates, IMPS Proxy Accounts permissions, IMPS Connectors and API access, CX con configuration files, CX Bindings (javascript)
  - Triage & determine which errors require CA Support Tickets or 3rd party vendor for product or unknown issue. Spend no more than 10 minutes on each issue to triage.
  - Open internal tracking list for CA and non-CA support Tickets
    - Assign resources to issue to resolve or work the issue
    - Tickets should be
      - Resolved (date of fix and deployment to QA/Stage/Model Env. and then when to production Env.),
      - Postponed (low impact),
      - Marked for resolution in confirm service pack (low-medium impact)
      - Escalated for CA support if CA Support ticket resolution not feasible in project time (high impact)
      - Escalated for internal management if internal resources resolution not feasible in project time (high impact)
  - Active Monitoring of Provisioning Servers (eta), IAM CS (log4j), & Endpoint Logs (sa & ADS)

MANAGING & CORRECTING ERROR MESSAGES - 03

- **Impact: High Value / Medium Difficulty**
- Description: Create Goal of No Error Message(s) in SiteMinder Policy Server logs; SiteMinder Web Agent Logs; CA Directory router and DSA logs.
- Actions:
  - Identify all error messages, e.g. strings with “ERROR”
  - Categorize and count error messages
    - Infrastructure, e.g. OS, Java, Database, Network
    - Product, e.g IM support with version of Infrastructure
    - Business Logic, e.g. Web Access Logs; DSA/Router logs
  - Triage & determine which errors require CA Support Tickets or 3rd party vendor for product or unknown issue. Spend no more than 10 minutes on each issue to triage.
  - Open internal tracking list for CA and non-CA support Tickets
    - Assign resources to issue to resolve or work the issue
    - Tickets should be
      - Resolved (date of fix and deployment to QA/Stage/Model Env. and then when to production Env.),
      - Postponed (low impact),
      - Marked for resolution in confirm service pack (low-medium impact)
      - Escalated for CA support if CA Support ticket resolution not feasible in project time (high impact)
      - Escalated for internal management if internal resources resolution not feasible in project time (high impact)
  - Active Monitoring of SiteMinder Policy Server;SiteMinder Web Agent; CA Directory Router & DSA logs.

ADVANCE TRAINING

ADVANCE TRAINING - 01

- **Impact: High Value / Medium Difficulty**
- Description: Create a goal of building an IM Sandbox Environment for self-training and validation of use-cases by each business / technical analyst
- Actions:
  - Recommend client invest in and expand client's technical and business knowledge. Client's IM personnel will need to perform OJT (on-the-job-training) with a sandbox environment that emulates client's production environments on the user's laptop to gain further expertise with complex and integrated solutions.
    - Demonstrate the solutions;
    - Perform internal self-training on production use-cases;
    - Validate configurations prior to dev/production rollout;
    - Build documentation for upgrades.
    - Manage complexity integration testing
    - Achieve advance subject matter expertise that is not provided by current vendor training
  - Recommended specs for laptops to support virtualized sandbox images:
    - Laptop Specs - Minimal:
      - Architecture: x64 bit Dual Processor w/ Hyper-threading {either Intel i5/i7 or AMD comparative}
      - BIOS: Support VT (Virtualization Technology)
      - RAM: 8 GB RAM
      - OS: 64bit OS (Windows Server 2008 Standard / Windows 7 or 8 / Linux – Suse or CentOS or Ubutu)
      - Hard Drive: 2 x 500 GB 7200 RPM HDD {one drive for os/programs; other drive for vmware images/snapshots}
      - Video: Standard / As-Is
      - Network: Standard / As-Is (LAN/WiFi)
      - DVD-Rom: Standard / USB version plug-in
  - Laptop Specs - Recommended:
      - Architecture: x64 bit Quad Processor w/ Hyper-threading {either Intel i5/i7 or AMD comparative}
      - BIOS: Support VT (Virtualization Technology)
      - RAM: 16 GB RAM
      - OS: 64bit OS (Windows Server 2008 Standard / Windows 7 or 8 / Linux – Suse or CentOS or Ubutu)
      - Hard Drive: 1 x 500 GB SSD Drive + 1 x 1 TB GB 7200 RPM HDD {one drive for os/programs; other drive for vmware images/snapshots}
      - Video: Standard / As-Is
      - Network: Standard / As-Is (LAN/WiFi)
      - DVD-Rom: Standard / USB version plug-in

ADVANCE TRAINING - 02

- **Impact: High Value / Medium Difficulty**
- Description: Create process to cross training staff with broad base knowledge
- Actions:
  - Recommend 2-3 day courses (online) for databases (MS SQL/Oracle)
    - Command Line Interfaces (CLI) & Web Administration Console
    - 3rd party tools - Dbvisualizer
  - Recommend 2-3 day course (online) for LDAP/X500 Directories (Open LDAP/CA Directory)
    - LDAP CLI (ldapsearch/ldapmod) & LDAP Administrations tools
    - LDIF Format
    - 3rd party tools – Jxplorer, SoftTerra LDAPBrowser/Admin, Apache LDAP
  - Recommend 2-3 day course (online) for Web Application Servers (Jboss/WebSphere/WebLogic)
    - Community version Jboss
    - Developer edition WebSphere
    - Developer edition WebLogic
  - Recommend 1 day course (online) for building SSL certificates
    - Host based
      - Active Directory certs (TCP 636)
      - Web Server certs (HTTPS)
      - LDAPS certs (LDAPS)
  - Recommend 1 day course (online) for Log4J configurations and understanding logs
    - Log4J properties / xml files
  - Recommend 5 day course (online) for Java coding/decoding
    - JDGui tool to decompile Java class files
    - Build LAH/BLTH/EL
  - Recommend 3-4 day course (OJT) for CX connector / operational bindings
    - XML mapping to database / directory
    - Javascript coding for CX operational bindings
  - Endpoint knowledge
    - Build own Active Directory Domain/Forest with users/groups
    - Build own Exchange 2010 Mail Server with mailboxes
    - Build own LDAP directory with users/groups
    - Build own database tables with users/groups
    - Build own Linux/Unix server with users/groups
    - Research & Review SAP Modules (ECC/HR/GR); ACF2/RACF/TSS security; Lotus Notes; AS/400; HP-Non Stop; GoogleApps & SalesForce; Oracle Financials (Oracle Applications)

DEBUGGING/TUNING

LOGGING.JSP DEBUGGING

- Here are the list of loggers that I find very useful when debugging. (5 of the hundreds available) / I enabled all loggers for im=debug and ims=debug, exercised use-cases; and then sorted through the list. Note: If using parent loggers, there is the possibility of being "buried in the noise".
- These select loggers will provide the details of the business logic that has been created in IM. I have included some commentary and examples of what would be returned that has high value.
-
- **General**
- ims.tasktrack.custom=DEBUG
- - Provides the start of the TASK or EVENT state:
- - 2013-08-24 15:15:17,225 INFO [ims.tasktrack.custom] (http-0.0.0.0-8080-2) Entered execute for task ModifyIdentityPolicySet and step VALIDATION
- - 2013-08-24 15:15:17,229 INFO [ims.tasktrack.custom] (http-0.0.0.0-8080-2) Exiting execute
- - 2013-08-24 15:15:17,233 INFO [ims.tasktrack.custom] (http-0.0.0.0-8080-2) Entered execute for task ModifyIdentityPolicySet and step SUBMITTED
-
- **Bulk Loader / BLC / Feeder** {View how the BLC or Bulk Load task loads data into IME}
- im.feeder = DEBUG
-
- **PX Rules**
- ims.policyxpress = DEBUG
- - Provides the complete trail of PX rules being executed
- - On a quiet system, use this to document the process data flow between PX rules (combine with identity polices as needed)
- ims.jdbc.JDBCManagedObjectProvider=DEBUG
- - Provides the name of the PX Rule to # in DB
- - Provides the event for PX_WHEN: SELECT "PX_WHEN"."UNIQUE_NAME", "EVENTNAME", "TYPE", "STEP", "POLICYUN" FROM "PX_WHEN" WHERE "TYPE"=? AND "STEP"=? AND "EVENTNAME"=? AND "ENV_OID"=? (6,16,ModifyUser,1)
-
- **Identity Policies**
- ims.jdbc.JDBCManagedObjectProvider=DEBUG {Same logger as above}
- - Provides the name of Identity Policy: SELECT "IM_IDENTITY_POLICY_SET"."UNIQUE_NAME", "ENABLED", "DESCRIPTION", "CATEGORY", "FRIENDLYNAME", "MEMBERRULE", "CONTAINSCOMPLIANCE" FROM "IM_IDENTITY_POLICY_SET" WHERE "FRIENDLYNAME"=? AND "ENV_OID"=? (Test001,1)
- - Provides the event for PX_WHEN: SELECT "PX_WHEN"."UNIQUE_NAME", "EVENTNAME", "TYPE", "STEP", "POLICYUN" FROM "PX_WHEN" WHERE "TYPE"=? AND "STEP"=? AND "EVENTNAME"=? AND "ENV_OID"=? (6,16,ModifyUser,1)
- ims.llsdk.role.azengine=DEBUG
- - Provides the name of the Identity Policy used for a user:
- - 2013-08-24 15:15:46,741 DEBUG [ims.llsdk.role.azengine] (http-0.0.0.0-8080-1) PolicyEngine.getCurrentIdentityPolicySets - Found 1 matching policy sets for user uid=bugs,ou=people,o=DEMOCORP,c=AU
- - 2013-08-24 15:15:46,741 DEBUG [ims.llsdk.role.azengine] (http-0.0.0.0-8080-1) PolicyEngine.getCurrentIdentityPolicySets - Returning 1 matching and enabled policy sets for user uid=bugs,ou=people,o=DEMOCORP,c=AU
- - 2013-08-24 15:15:46,780 DEBUG [ims.llsdk.role.azengine] (http-0.0.0.0-8080-1) PolicyEngine.getCurrentIdentityPolicies - Check for preventative identity policies. Identity policy set 'Test001' contains 1 policies
- - 2013-08-24 15:15:46,780 DEBUG [ims.llsdk.role.azengine] (http-0.0.0.0-8080-1) PolicyEngine.getCurrentIdentityPolicies - Found 0 preventative identity policies in the identity policy set 'Test001'
- ims.llsdk.role.azcache.ridiculouslydetailed=DEBUG
- - Provide detail on Identity Policy
- - 2013-08-24 15:15:47,881 DEBUG [ims.llsdk.role.azcache.ridiculouslydetailed] (WorkManager(2)-37) Testing directory policy for user uid=bugs,ou=people,o=DEMOCORP,c=AU with rule [<MemberRule><AttributeExpression attribute="postalAddress" comparator="EQUALS" value="1"/></MemberRule>]
- - 2013-08-24 15:15:47,888 DEBUG [ims.llsdk.role.azcache.ridiculouslydetailed] (WorkManager(2)-37) User uid=bugs,ou=people,o=DEMOCORP,c=AU matches directory rule [<MemberRule><AttributeExpression attribute="postalAddress" comparator="EQUALS" value="1"/></MemberRule>]
- - 2013-08-24 15:15:47,888 DEBUG [ims.llsdk.role.azcache.ridiculouslydetailed] (WorkManager(2)-37) Finished calculating 1 directory policies for user bugs
-
-
- **JDBC** (To see ALL jdbc calls, then the parent logger may be used.)
- ims.jdbc =DEBUG

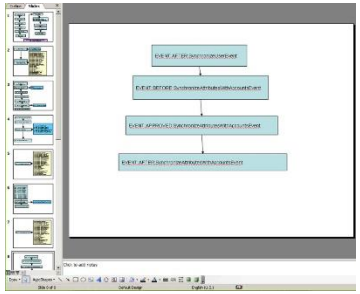
TUNING GUIDELINES FROM CA BOOKSHELVES

- Continually monitor the latest IM/SM/Dir/AM/RM bookshelves for new updates
  - Search on keywords of “tune”, “performance”, “pool”, “index”
  - Example:
    - Search of “tune”
      - Returned 13 results for IM r12.6sp2
      - Returned 12 results for SM r12.5
      - Returned 1 results for Dir r12.0sp11
      - Returned 10 results for AM 7.1/RM r3.1
    - Search of “performance”
      - Returned 14 results for IM r12.6sp2
      - Returned 107 results for SM r12.5
      - Returned 60 results for Dir r12.0sp11
      - Returned 61 results for AM 7.1/RM r3.1
    - Search of “pool”
      - Returned 36 results for IM r12.6sp2
      - Returned 18 results for SM r12.5
      - Returned 0 results for Dir r12.0sp11
      - Returned 86 results for AM 7.1/RM r3.1
    - Search of “index”
      - Returned 18 results for IM r12.6sp2
      - Returned 37 results for SM r12.5
      - Returned 16 results for Dir r12.0sp11
      - Returned 31 results for AM 7.1/RM r3.1

DOCUMENT IM BUSINESS LOGIC

DOCUMENT IM BUSINESS LOGIC

- Goal: Documentation of IM business logic.
- Business logic may change during the lifecycle of the solution. And as it drifts from initial documentation, it can be a costly process for debugging or adding on new functionality without impacting current business. The process outline below will demonstrate a step by step process of how to capture business logic and then document within MS powerpoint or MS visio for a complete view of all uses cases.
- This process may be time consuming and will require a pre-prod environment that has matching prod business logic.
- The pre-prod system MUST be quiet; which mean no other users or services acting upon the solution during this process; otherwise "noise" will defeat this exercise.
- **Actions:**
  - Deploy the IM logging.jsp process from the CA IM samples (IAM Suite / Tools) to ALL J2EE platforms.
    - Copy this file over the existing STUB jsp with the same name.
    - Recompile for JBOSS (Not required for WebLogic/WebSphere)
  - Launch the browser to the URI with logging.jsp to ALL J2EE servers (or just run one J2EE) (E.g http://imwa001.im.dom:7001/iam/im/logging.jsp)
  - Enabled the following
    - J2EE loggers to DEBUG state {be careful of spaces}
      - **ims.tasktrack.custom** {Used to monitor general start/exit transition for task/event/blth/lah}
      - **im.feeder** {View how the BLC or Bulk Load task loads data into IME}
      - **ims.policyxpress** {Provides the complete trail of PX rules being executed}
      - **ims.llsdk.role.azengine** {Provides the name of the Identity Policy used for a user}
      - **ims.llsdk.role.azcache.ridiculouslydetailed** { Provide detail on Identity Policies executed}
    - IMPS ETAtrans logs (loglevel=**3**) (IMPS\logs\etatrans{datestamp}.log)
    - IMPS ADS log (IMPS\logs\ADS\adshostname.log)
    - If needed; {IMPS Exchange Logs ((IMPS\logs\ADS\adshostname.log) + IMPS CAM Logs (CAM\logs*)



  - Note the time stamp before starting
    - Validate the J2EE logs are quiet
    - If other loggers are present, and are "noisy"; set that logger = WARN in logging.jsp during this exercise.
  - Execute the beginning of the use-case
    - If using the IM Bulk Loader Client; execute that process for one (1) record pre use-case.
      - Do not use more than one; as this will add "noise" and make it difficult to map the business logic.
  - Monitor the progress of the use-case with IM View Submitted Task
    - When the task shows as "completed", view the J2EE log and ensure that all loggers are viewable, ensuring that they were entered correctly within the logging.jsp.
    - If all loggers are seen, copy this file to your desktop.
  - Open Visio or PowerPoint or any tool that will allow a capture of visual representation of the data flow.
    - Create a starting point with the 1st box; it will be labeled with the very first STEP of the [ims.policyxpress] logger. **TASK:STARTED:ObjectsFeeder**
    - Continue to the next STEP of the [ims.policyxpress] logger; add in arrows between the boxes of the serial data flow.
    - When a STEP has a PX rule executed; identify the step; then add another box (comment) to the side that captures the PX Rule's name
      - Additional information of the PX rule will need to wait, until we capture the entire serial data process flow.
    - This process will continue across multiple slides, as needed, don't crowd the data, as additional information will be added later, to fill out the business logic executed.
    - Create a new deck or visio TAB for each use-case.
    - After the process flow has been captured for each STEP, add in additional notes on PX Rule priorities & PX Action Rules.
      - PX Data Elements (with loops) + PX Action Rules will have their own data flow (Iterators)
      - Multiple PX Rule may exist for the SAME STEP, e.g. priority 10,20,30,40,…,999.
      - Capture the PX data flow on a new deck/visio.
    - If business logic is missing due to BLTH or other custom code; add in these loggers as needed, and re-execute the use-case.
  - Review of business logic
    - Follow PX Framework best practices (see the CA Community Site for the PX Wiki) to move any PX Rule trigger from an EVENT STEP to a TASK STEP.
    - Identify any IM Identity Policies that may be moved to PX Framework
    - Determine if any PX Rule may be adjusted with Data Entry Rule to prevent execution for use-cases that don't apply.
    - Remember to add the IMPS provisioning logs from ETA/ADS/Exchange/CAM to complete the data flow.